Grupos. Subgrupos. El Terorema de Lagrange. Grupo cociente. Teoremas de Isomorfía

Título: Grupos. Subgrupos. El Terorema de Lagrange. Grupo cociente. Teoremas de Isomorfía. **Target**: Profesores de matemáticas. **Asignatura**: Algebra. **Autor**: Maria de la O Martinez Santibañez, Licenciada en Matematicas, Profesora de Matematicas en Educacion Secundaria.

El nacimiento del Álgebra fue uno de los grandes avances de la matemática, ya que por medio de la abstracción consistente en sustituir números por letras podían liberarse de resolver problemas concretos para estudiar familias de problemas. A partir de un cierto conjunto de elementos, de ciertas leyes de composición y de la verificación de unas propiedades concretas se obtiene el concepto de *Estructura Algebraica*.

En este tema vamos a estudiar una de esas estructuras, la de *grupo*. Estudiaremos algunas de sus propiedades y conceptos básicos. Estudiaremos los subgrupos, analizaremos los cardinales de los subgrupos, grupos cociente y ciertos subconjuntos de un grupo G en función del cardinal de G, ya que cuando G es finito, éstos cardinales juegan un papel esencial en el análisis de la estructura del grupo G a través de los subgrupos y grupos cocientes propios de G. El estudio de este tema es importante ya que la teoría de grupos es útil, entre otros campos, en el diseño de sumadores rápidos y de códigos de corrección, así como constituir una base sobre la que se sustenta toda la teoría de códigos y criptografía.

1. Operaciones binarias. Grupos.

Definición: Sea $G \neq \varnothing$ un conjunto dotado de una operación binaria interna $\boxed{\begin{array}{l} *: G \times G \to G \\ \quad (a,b) \to a*b = ab \end{array}}$

- Se dice que $(G,*)$ es un semigrupo si $*$ es asociativa.
- Se dice que $(G,*)$ es un monoide si es un semigrupo y $\exists e \in G \ \ tal \ \ que \ \ e*a = a*e = a \quad \forall a \in G$.
- Se dice que $(G,*)$ es un grupo si es un monoide y cada elemento del conjunto posee inverso, es decir, $\forall a \in G, \quad \exists a' \in G \quad tal \ que \quad a*a' = a'*a = e$.

Así que, podemos definir,

Definición: Se dice que el par formado por $(G,*)$ es un grupo, con $G \neq \varnothing$ y $*$ operación binaria interna, si se verifica:

i) $\forall a,b,c \in G \quad se \ cumple \quad a*(b*c) = (a*b)*c \quad (asociatividad)$.

ii) $\exists e \in G \ \ tal \ \ que \ \ e*a = a*e = a \quad \forall a \in G \qquad (e \ \ elemento \ neutro)$

iii) $\forall a \in G, \quad \exists a^{-1} \in G \quad tal \ que \quad a*a^{-1} = a^{-1}*a = e \qquad (a^{-1} \ \ elemento \ simétrico)$

Si se verifica que $\forall a,b \in G, \quad a*b = b*a$, se dice que $(G,*)$ es un grupo abeliano o conmutativo.

Notas:

1) Si se sobreentiende la operación binaria $*$ en G, de modo que $(G,*)$ es un grupo, diremos simplemente que G es un grupo.

2) $(G,*)$ es un grupo finito si G es finito.

Ejemplos:

1) $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ son grupos abelianos $\left(e=0 \quad , \quad a^{-1}=-a\right)$.

2) $(\mathbb{Q}-\{0\},\times),(\mathbb{R}-\{0\},\times),(\mathbb{C}-\{0\},\times)$ son grupos abelianos $\left(e=1 \quad , \quad a^{-1}=\frac{1}{a}\right)$.

3) $(\mathbb{Z}-\{0\},\times)$ no es grupo, pues falla la condición ii).

4) V k-espacio vectorial, $(V,+)$ es un grupo abeliano.

5) Sea $n\in\mathbb{Z}^+$ y consideramos $\mathbb{Z}_n=\{\bar{0},\bar{1},\ldots,\overline{n-1}\}$ (*clases de residuos módulo n*) o clases de equivalencia, al considerar en $\mathbb{Z}$ la relación de equivalencia: $\boxed{a\sim b \iff a-b\in n\mathbb{Z}}$ (donde las clases son $\bar{a}=a+n\mathbb{Z}$), se tiene que $\boxed{(\mathbb{Z}_n,+)}$ es un grupo abeliano $\left(e=\bar{0} \quad , \quad \bar{a}^{-1}=\overline{-a}\right)$, siendo $\boxed{\begin{array}{c}+:\mathbb{Z}_n\times\mathbb{Z}_n\to\mathbb{Z}_n\\ (\bar{a}\ ,\ \bar{b})\to\bar{a}+\bar{b}=\overline{a+b}\end{array}}$.

Sin embargo, si consideramos $\boxed{(\mathbb{Z}_n,\bullet)}$ no es grupo abeliano. Pero, considerando en $\mathbb{Z}_n$ todos los elementos que son inversibles, $\boxed{\mathbb{Z}_n^{\times}=\{\bar{a} \mid mcd(a,n)=1\}}$ con la operación $\boxed{\begin{array}{c}\bullet:\mathbb{Z}_n^{\times}\times\mathbb{Z}_n^{\times}\to\mathbb{Z}_n^{\times}\\ (\bar{a}\ ,\ \bar{c})\to\bar{a}\bullet\bar{c}=\overline{ac}\end{array}}$, se sabe que $\exists c,d\in\mathbb{Z} \quad tales\ que \quad ac+nd=1$ y así $\bar{a}\bullet\bar{c}=\bar{1}$ (porque $ac-1\in n\mathbb{Z}$). Entonces, $(\mathbb{Z}_n^{\times},\bullet)$ es un grupo abeliano.

Proposición (Reglas de cálculo)

Sea $(G,*)$ un grupo. Se tiene:

i) El elemento neutro es único.

ii) El elemento inverso de $a\in G$, a^{-1},es único

iii) $\left(a^{-1}\right)^{-1}=a$

iv) $(a*b)^{-1}=b^{-1}*a^{-1}$

Observaciones:

1) En adelante, la operación de grupo la denotaremos por $\bullet$, y en ocasiones $a\bullet b$ lo denotaremos por ab.

2) Sea $n\in\mathbb{Z}^+$ y G un grupo, con $a\in G$. Entonces $\boxed{a^n=\overbrace{a\cdot a\cdot a\cdot\ldots\cdot a}^{(n-veces}}$, $\boxed{a^{-n}=\overbrace{a^{-1}\cdot a^{-1}\cdot a^{-1}\cdot\ldots\cdot a^{-1}}^{(n-veces}}$ y $\boxed{a^0=e}$.

3) A partir de ahora, el elemento neutro lo denotaremos por *1*.

4) Si G es un grupo abeliano, la operación se denotará por +. Si $n\in\mathbb{Z}^+$, entonces $na=\overbrace{a+\ldots+a}^{(n}$ y $-na=\overbrace{(-a)+\ldots+(-a)}^{(n}$, donde $(-a)$ denota el opuesto de *a*. El elemento neutro de G se denota por 0 y $0a=0$.

Proposición Si *G* es un grupo y $a,b\in G$, entonces $\exists|x\in G \quad t.q. \quad ax=b$ y $\exists|y\in G \quad t.q. \quad ya=b$. En consecuencia,

i) Si $au=bu \implies a=b$

ii) Si $va=vb \implies a=b$

iii) Si *G* es finito, para cada $x\in G$, $\exists n\in\mathbb{N} \quad t.q. \quad x^{-1}=x^n$.

Definición: Sea *G* un grupo y sea $x\in G$. El menor entero positivo $n\in\mathbb{Z}^+$ tal que $x^n=1$, se dice orden de *x* y se denota $|x|$. Si tal entero no existe, se dice que *x* tiene orden infinito.

Ejemplos:
1) El elemento neutro es el único que tiene orden 1.
2) En $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ todos los elementos tienen orden infinito, salvo el neutro.
3) En $(\mathbb{Q}-\{0\},\times),(\mathbb{R}-\{0\},\times),(\mathbb{C}-\{0\},\times)$, el 1 tiene orden 1 y (-1) tiene orden 2. Los demás, tienen orden infinito.
4) En $(\mathbb{Z}_9,+)$, el orden de $\overline{6}$ es 3 y el orden de $\overline{5}$ es 9.

Definición: Sea *G* un grupo. Definimos el orden de *G* como el número de elementos que tiene, y se denota $orden\ de\ G = |G|$.

2. Subgrupos.
Definición: Sea *G* un grupo y sea $H \subseteq G$. Se dice que *H* es un subgrupo de *G* si $H \neq \emptyset$ y *H* es cerrado por productos y por inversos, es decir, $\forall x,y \in H$, $xy \in H$ y $x^{-1} \in H$. Se denota $\boxed{H \leq G}$.
Nota: $1_G = 1_H = 1$ y $(x^{-1})_H = (x^{-1})_G = x^{-1}$ siempre.
Observaciones:

1) Si $H \leq G$, entonces $(H,\bullet)$ es un grupo.
2) Nótese que si $H \leq G$, entonces $1 \in H$, $x^{-1} \in H$ *si* $x \in H$.
3) Si $H \leq G$ y $H \neq G$, se denota $H < G$.
4) Si $K \leq H$ y $H \leq G$, entonces, $K \leq G$ (transitividad).

Ejemplos:
1) Si *G* es un grupo, *{1}* y *G* son subgrupos de *G* y se llaman subgrupos triviales.
2) $(\mathbb{Z},+) \leq (\mathbb{Q},+)$ y $(\mathbb{Q},+) \leq (\mathbb{R},+)$
3) $(2\mathbb{Z},+) \leq (\mathbb{Z},+)$
4) No son subgrupos: $(\mathbb{Z}^+,+)$ no es subgrupo de $(\mathbb{Z},+)$ y $(\mathbb{Z}-\{0\},\times)$ no es subgrupo de $(\mathbb{Q}-\{0\},\times)$.

Proposición (Criterio de caracterización de subgrupos)
Sea *G* grupo y $H \subseteq G$. Entonces,

i) $H \leq G \iff H \neq \emptyset$ y $\forall x,y \in H$, $xy^{-1} \in H$
ii) Si *G* es finito, $H \leq G \iff \forall x,y \in H$, $xy \in H$

Dem:
i) $\Rightarrow$ Clara, pues si $y \in H \to y^{-1} \in H$ y entonces $xy^{-1} \in H$, $\forall x \in H$, pues *H* es subgrupo.
$\Leftarrow$ $H \neq \emptyset$ por hipótesis. Veamos si $\forall x,y \in H$ ¿$xy \in H$, $x^{-1} \in H$?
Como $H \neq \emptyset$, sea $x \in H$ y ahora por hipótesis, $xx^{-1} = 1 \in H$. Ahora, dados $x \in H$, como $1, x \in H$ (por hip), $1x^{-1} = x^{-1} \in H$. Si $x,y \in H$, como $y^{-1} \in H$, entonces $x, y^{-1} \in H$ y por hipótesis $x(y^{-1})^{-1} = xy \in H$. ■
ii) $\Rightarrow$ Trivial
$\Leftarrow$ Basta con ver que $xy^{-1} \in H$, $\forall x,y \in H$ y aplicar i). $y \in H \overset{G\ finito}{\Rightarrow} y^{-1} = y^m\ con\ m \in \mathbb{N}$. Luego,
$xy^{-1} = x\underbrace{(y \cdots y)}_{m} = \underbrace{(xy)}_{\in H\ hip} y^{m-1} = \underbrace{(xy)y}_{\in H\ hip} y^{m-2} = \ldots = xy^{-1} \in H$. Como $xy^{-1} \in H \underset{i)}{\Rightarrow} H \leq G$. ■

Observación: ii) no es cierto si *G* es infinito. *Ejemplo*: $(\mathbb{N},+)\subseteq(\mathbb{Z},+)$ y $\forall n,m\in\mathbb{N}\quad,\quad n+m\in\mathbb{N}\ y\ \mathbb{N}\not\leq\mathbb{Z}$.

Proposición

i) La intersección arbitraria de subgrupos es siempre subgrupo.

ii) Sea $\varnothing\neq H\subseteq K\leq G$. Entonces, $H\leq G \iff H\leq K$.

iii) $H,K\leq G$. Entonces, $H\cup K\leq G \iff H\subseteq K \quad ó \quad K\subseteq H$

iv) $H,K\leq G$. Entonces, $HK:=\{hk\,|\,h\in H,k\in K\}$ y $KH:=\{kh\,|\,k\in K,h\in H\}$. Se tiene que $HK\leq G \iff HK=KH \iff KH\leq G$

Definición: sea $(G,\bullet)$ grupo y $\varnothing\neq S\subseteq G$. Al menor subgrupo de *G* conteniendo a *S*, que además es subgrupo de G, se le denomina subgrupo generado por *S* *ó* generador de *S* y se le denota $\langle S\rangle=\bigcap\{H\leq G\,|\,S\subseteq H\}$.

Observación:

- Si $S=\{x_1,x_2,\ldots,x_k\} \Rightarrow \langle S\rangle=\langle x_1,\ldots,x_k\rangle$ y se dice que $\langle S\rangle$ es finitamente generado.
- Si $S=\{x\} \Rightarrow \langle S\rangle=\langle x\rangle=\{x^n\,|\,n\in\mathbb{Z}\}$ y en este caso diremos que $\langle S\rangle$ es cíclico con generador *x*.
- En general, si un grupo *G* verifica: $\exists\, x\in G \quad t.q \quad G=\langle x\rangle$, se dice que *G* es grupo cíclico.
- Si $|G|=1,2\ ó\ 3 \Rightarrow$ *G* es cíclico.
- Los subgrupos de un grupo forman lo que se conoce como retículo de subgrupos de un grupo.

Ejemplo: en $\mathbb{Z}_4$ hay subgrupos de orden $d\,|\,4\Rightarrow \quad d=1,2,4$ y se representan así

$\langle 1\rangle=\langle 3\rangle$
$\langle 2\rangle$
$\langle 0\rangle$

Proposición Sea $G=\langle x\rangle$, *G* grupo multiplicativo.

i) Si $|G|=n \Rightarrow G\cong(\mathbb{Z}_n,+)$

ii) Si G es infinito $\Rightarrow G\cong(\mathbb{Z},+)$

3. El Teorema de Lagrange.

Definición: Sea $(G,\bullet)$ grupo y sea $H\leq G$. Para cada $x\in G$ se define:

- Clase a izquierda del elemento x: $xH=\{xh\,|\,h\in H\}$
- Clase a derecha del elemento x: $Hx=\{hx\,|\,h\in H\}$

En general, $Hx\neq xH$ y que $Hx=xH$ no significa que $xh=hx$ sino que $\Leftrightarrow\begin{cases}\forall h\in H \quad \exists h' \quad t.q. \quad xh=h'x\\ \forall h'\in H \quad \exists h'' \quad t.q. \quad h'x=xh''\end{cases}$

Propiedades Elementales

1) $x\in Hx,xH \quad (x=x\cdot 1\in xH \quad ; \quad x=1\cdot x\in Hx)$ y $\begin{matrix}H\to Hx\\ h\to hx\end{matrix}$, $\begin{matrix}H\to xH\\ h\to xh\end{matrix}$ aplicaciones biyectivas, luego $|xH|=|Hx|=|H|$. En particular, $G=\bigcup_{x\in G}xH=\bigcup_{x\in G}Hx$

2) $\boxed{x\in H \iff Hx=xH=H}$

3) $\forall x,y\in G \quad , \quad \begin{cases}yH=xH\\ \quad ó \\ yH\cap xH=\varnothing\end{cases}$. En particular, $\begin{cases}x\in yH \iff xH=yH\\ x\in Hy \iff Hx=Hy\end{cases}$

4) Número de clases a izquierda módulo *H* = Número de clases a derecha módulo *H*

Nuestro *objetivo* ahora es poder descomponer el grupo G como unión disjunta de clases a derecha o a izquierda de tal forma que en cualquiera de las descomposiciones se tenga el mismo número de elementos. Para ello son necesarias las definiciones siguientes.

Definición: dado $H \leq G$, una familia de elementos de *G* $\{x_i\}_{i\in I}$, exactamente uno por cada clase distinta a izquierda, se dice sistema completo de representantes de clases a izquierda módulo H (análogamente sistema completo de representantes de clases a derecha módulo H) si $\left.\begin{cases} i)\ x_iH \cap x_jH = \varnothing \quad i \neq j \\ ii)\ G = \bigcup_{i\in I} x_iH \end{cases}\right\} \Leftrightarrow \boxed{G = \dot{\bigcup_{i\in I}} x_iH}$

Definición: sea $H \leq G$, llamaremos índice de *H* en *G* y se denota $[G:H]$ al número de clases a izquierda distintas que hay en *G* ó equivalente al número de clases a derecha distintas que hay en *G*.

Así que $\boxed{G = \dot{\bigcup_{i\in I}} x_iH} \Leftrightarrow [G:H] = |I|$, luego si *G* finito y $H \leq G \Rightarrow$ *H* finito y $|xH| = |Hx| = |H|$, $\{x_i\}_{i\in I}$ sistema completo de representantes de clases a izquierda $\Rightarrow I$ finito y $|I| = [G:H] = r \Rightarrow$ $\boxed{G = \dot{\bigcup_{1\leq i\leq r}} x_iH} \Rightarrow |G| = \sum_{i=1}^{r} |x_iH| = \sum_{i=1}^{r} |H| = r|H| = [G:H]\cdot|H|$.

Teorema de Lagrange

Sea *G* finito y $H \leq G$. Entonces, $|H|\,||G|$ y el número de clases a izquierda es $\dfrac{|G|}{|H|}$.

Dem: Sabemos que $G = g_1H \dot{\cup} \ldots \dot{\cup} g_sH$, donde $g_1H, \ldots, g_sH$ son las clases a izquierda distintos que hay.

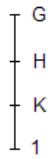
Además $\begin{matrix} H \longleftrightarrow g_iH \\ h \longrightarrow g_ih \end{matrix}$ es suprayectiva e inyectiva $\left(g_ih = g_ih' \xrightarrow{\cdot g_i^{-1}} h = h'\right)$, luego biyectiva.

Así que $|G| = |H| \overset{(s\ veces)}{+ \cdots +} |H| = s\cdot|H|$ y por tanto $|H|\,||G|$ y el número de clases a izquierda es $s = \dfrac{|G|}{|H|}$. ■

Aplicaciones:

1) Si *G* es finito $\Rightarrow \boxed{[G:H] = \dfrac{|G|}{|H|}} \Rightarrow |G| = [G:H]\cdot|H| = [G:H]\cdot[H:1]$, ya que $\{1\} \leq G, H$.

2) Dados $K \leq H \leq G \Rightarrow [G:K] = [G:H]\cdot[H:K]$ (Transitividad del índice)



3) Si *G* es infinito y $H \leq G$, puede ocurrir lo siguiente:

Ejemplo:

$|\mathbb{Z} : \{0\}| = \infty$, hay infinitas clases a izquierda, elementos de $\mathbb{Z}/\{0\}$, y $|\mathbb{Z} : n\mathbb{Z}| < \infty$, hay *n* elementos de $\mathbb{Z}/n\mathbb{Z}$.

4) Los subgrupos de un grupo finito tienen por número de elementos un divisor del orden del grupo.

5) Si *G* es finito, $\forall x \in G$, $|x|\,||G|$. En particular, $x^{|G|} = 1$

6) Los grupos de orden primo son cíclicos.

4. Grupo cociente.

Nuestro propósito a lo largo de este apartado es encontrar lo subgrupos que denominaremos "buenos" para poder definir un grupo cociente.

Definición: dados un grupo *G* y $H \leq G$, definimos en *G* las siguientes relaciones de equivalencia:

a) $\boxed{x \equiv_i y \pmod{H} \iff y^{-1}x \in H}$

b) $\boxed{x \equiv_d y \pmod{H} \iff xy^{-1} \in H}$

Además,

$[x]_{\equiv_i} = xH$. En particular, $xH = yH \iff x \equiv_i yH \iff y^{-1}x \in H$

$[x]_{\equiv_d} = Hx$. En particular, $Hx = Hy \iff x \equiv_d yH \iff xy^{-1} \in H$

Proposición (Caracterización de subgrupos normales)

Sea *G* grupo y $H \leq G$, son equivalentes:

i) $\forall x \in G, \quad x^{-1}Hx \subseteq H$

ii) $\forall x \in G, \quad xH = Hx$

iii) $\forall a,b,c,d \in G \quad t.q. \quad \begin{cases} aH = cH \\ bH = dH \end{cases} \Rightarrow (ab)H = (cd)H$, es decir, la relación de congruencia (a izquierda) módulo *H* es compatible con la operación producto del grupo *G*.

Dem:

$i) \Rightarrow ii)$ Dado $x \in G$,

$$\xrightarrow[hip]{} \begin{cases} x^{-1}hx \subseteq H \Rightarrow Hx \subseteq xH \\ x^{-1} \in G \xrightarrow[hip]{} \left(x^{-1}\right)^{-1} Hx^{-1} = xHx^{-1} \subseteq H \Rightarrow xH \subseteq Hx \end{cases} \Rightarrow Hx = xH \ . \blacksquare$$

$ii) \Rightarrow iii)$

$$(ab)H = a(bH) \underset{\left(bH \underset{hip}{=} Hb\right)}{=} a(Hb) = (aH)b = (cH)b = c(Hb) = c(bH) = c(dH) = (cd)H \ . \blacksquare$$

$iii) \Rightarrow i)$ En general, dados a, b, c, d $\in$ G, verificando $\left.\begin{matrix} aH = cH \\ bH = dH \end{matrix}\right\} \underset{hip}{\Rightarrow} (ab)H = (cd)H$, se tiene que

$aH = cH \iff c^{-1}a \in H$, $bH = dH \iff d^{-1}b \in H$ y

$(ab)H = (cd)H \iff (cd)^{-1}ab \in H \iff d^{-1}c^{-1}ab \in H$.

Sea ahora, $a^{-1}c^{-1}ab = \underbrace{d^{-1}c^{-1}ad}_{\in H} d^{-1}b \in H \Rightarrow d^{-1}c^{-1}ad \in H$. Sea $c \in H$, luego $c^{-1} \in H$ y $c^{-1}H = 1 \cdot H = H$.

$d^{-1}cd = d^{-1}\left(c^{-1}\right)^{-1} d \in H$ (válido $\forall c \in H$), luego $d^{-1}Hd \subseteq H$. $\blacksquare$

Definición: un subgrupo *H* de un grupo *G* se dice normal y se denota $\boxed{H \lhd G}$, si verifica una cualquiera de la condiciones equivalentes anteriores.

Si $\boxed{H \lhd G}$, denotamos $\boxed{G/H = G/\equiv = \{xH \mid x \in G\}}$ y tenemos que $\left|G/H\right| = [G:H]$ y además la operación

$(xH)(yH)=(xy)H$ está bien definida (gracias a iii) de la proposición anterior) y hace que G/H tenga estructura de grupo.

Definición: $\boxed{G/H}$ es el grupo cociente de *G* módulo *H.*

La siguiente proposición nos da una condición para determinar los subgrupos $H \leq G$ con los que es posible definir el grupo cociente G/H.

Proposición Sea $H \leq G$, entonces,

$$H \lhd G \quad \Leftrightarrow \quad H \text{ es el núcleo de un homomorfismo,} \quad H = Ker\ f \quad , \quad f \quad \text{homomorfismo}$$

Ejemplos importantes:

Observamos que si $\boxed{H \lhd G}$, la aplicación $\begin{matrix} p: G \to G/H \\ x \to xH \end{matrix}$ es un epimorfismo de grupos.

1) $Ker\ f = \{x \in G \mid xH = H\}$, $\forall f: G \to G'$ homomorfismo de grupos, $Ker\ f \lhd G$.

2) Si *G* es abeliano, $H \lhd G \quad \forall H \leq G$.

3) $H = \langle x \rangle \leq G$, $H \lhd G \quad \Leftrightarrow \quad y^{-1}xy \in H$

4) La intersección arbitraria (finita o no) de subgrupos normales es subgrupo normal.

OJO! $H \lhd K \lhd G \quad \not\Rightarrow \quad H \lhd G$, ahora si $H \lhd G \quad y \quad K \lhd G \quad t.q. \quad H \subseteq K \quad \Rightarrow \quad H \lhd K$

Antes de pasar al siguiente apartado, vamos a ver la siguiente proposición que nos va a decir cómo son los subgrupos de grupos cociente.

Proposición Sea *G* grupo, $H, K \leq G \quad t.q. \quad H \supseteq K \lhd G$, entonces $H^* = H/K \leq G/K = G^*$, es más,

i) $*: \{H \leq G \mid K \subseteq H\} \longrightarrow \{subgrupos\ G/K\}$ definida por $H^* = p(H) = H/K$ es biyectiva ($p: G \longrightarrow G/K$ proyección canónica)

ii) $H^* \lhd G^* \quad \Leftrightarrow \quad H \lhd G$

5. Teoremas de Isomorfía.

Sean $(G,\bullet)$ y $(G',\bullet)$ grupos, donde representamos las operaciones internas por el mismo símbolo por razones de escritura y comodidad.

Definición: una aplicación *f* del conjunto *G* en el conjunto *G'* es un homomorfismo si y sólo si $f(xy) = f(x)f(y) \quad \forall x, y \in G$.

- Si *f* es inyectiva, se dice que es un monomorfismo.
- Si *f* es sobreyectiva, se dice que es un epimorfismo.
- Si *f* es biyectiva, se dice que es un isomorfismo.
- Si *G=G'*, un homomorfismo *f* de *G* en *G*, recibe el nombre de endomorfismo.
- Si *G=G'*, un isomorfismo *f* de *G* en *G*, recibe el nombre de automorfismo de *G*.

TEOREMA (1ER Teorema de Isomorfía)

Sea $f:G\to H$ homomorfismo de grupos $\Rightarrow$ $\boxed{G/_{Ker\ f}\approx \mathrm{Im}\ f}$

Dem:
El siguiente cuadro es conmutativo:

$$\begin{array}{ccc} G & \xrightarrow{\ f\ } & H \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ G/_{Ker\ f} & \xrightarrow{\ f^*\ } & \mathrm{Im}\ f \\ xKer\ f & \longrightarrow & f(x) \end{array}$$

Se define $f^*: G/_{Ker\ f}\to \mathrm{Im}\ f$, como $f^*\left(xKer\ f\right)=f(x)$. Veamos que f^* es isomorfismo. Se tiene que,

- f^* está bien definida y es inyectiva:

$$xKer\ f=yKer\ f \iff y^{-1}x\in Ker\ f \iff f\left(y^{-1}x\right)=f(y)^{-1}f(x)=1 \iff f(x)=f(y)$$

- f^* es homomorfismo:

$$f^*\left(\left(xKer\ f\right)\left(yKer\ f\right)\right)=f(xy)=f(x)f(y)=f\left(xKer\ f\right)f\left(yKer\ f\right)$$

- f^* es sobreyectiva, así que f^* es isomorfismo.■

Definición: sea $\varnothing\neq S\subseteq G$, se define normalizador en G de S y se denota $N_G(S)$ a $N_G(S)=\{x\in G\mid xS=Sx\}=\{x\in G\mid x^{-1}Sx=S\}$. Se tiene que $N_G(S)\leq G$

TEOREMA (2NDO Teorema de Isomorfía)

Sean $K,H\leq G$ $t.q.$ $K\subseteq N_G(H)$ $\Rightarrow$ $\boxed{HK/_H\approx K/_{K\cap H}}$

Dem: Como $K\subseteq N_G(H)$, se tiene que $H\lhd HK=KH$ y $K\cap H\lhd K$.
Definimos

$\left(K\subseteq KH=HK\right)$: $f: K\xrightarrow{\ i\ } KH\xrightarrow{\ p\ } KH/_H$
$k\longrightarrow k\longrightarrow kH$

. que es epimorfismo de grupos (es composición de homomorfismos y además si $a\in KH/_H$, $a\underset{k\in K,h\in H}{=}(kh)H=k(hH)=kH$, luego $f(k)=a$, lo que prueba que es sobreyectiva).
Calculamos ahora $Ker\ f$:
$Ker\ f=\{k\in K\mid kH=H\}=\{k\in K\mid k\in H\}=H\cap K$, luego aplicando el 1er Teorema de Isomorfía tenemos el resultado. $K/_{Ker\ f}\approx K/_{K\cap H}\approx \mathrm{Im}\ f\approx KH/_H$. ■

TEOREMA (3ER Teorema de Isomorfía)

Sean $K,H\lhd G$ $t.q.$ $K\subseteq H$ (luego $K\lhd H$) $\Rightarrow$ $H/_K\lhd G/_K$ y $\boxed{G/_K\Big/_{H/_K}\approx G/_H}$

Dem: Se tiene que $H/_K\lhd G/_K$ por las propiedades que verifican los subgrupos de grupos cociente al ser $K,H\lhd G$ y $K\lhd H$.

Definimos ahora $g : {G}/{K} \to {G}/{H}$, $xK \to xH$. Se tiene que $xK = yK \Leftrightarrow y^{-1}x \in K \subseteq H \Rightarrow xH = yH$, y por tanto g es aplicación, es más, es epimorfismo de grupos. Además, $Ker\ g = \left\{ xk \mid xH = 1_{{G}/{H}} = H \right\} = \left\{ xk \mid x \in H \right\} = {H}/{K}$. luego aplicando el 1er Teorema de Isomorfía tenemos el resultado. ${\left({G}/{K}\right)}/{Ker\ g} \approx {\left({G}/{K}\right)}/{\left({H}/{K}\right)} \approx {G}/{H}$. ■

6. Conclusión.

Para terminar y como conclusión podemos decir que el álgebra desde la antigüedad ha constituido una parte esencial de las matemáticas. Como cito *Sofía Germain* (S XIX) "el álgebra no es otra cosa que la geometría expresada en símbolos y la geometría es álgebra expresada en figuras" .

En nuestros días, no sin fundamento, se habla de "*algebraización*" de las matemáticas, y en correspondencia con el principio de que "lo importante no son los objetos matemáticos sino las relaciones entre ellos", el álgebra se define como ciencia de las operaciones algebraicas, efectuadas sobre los elementos de diferentes conjuntos. Las propias operaciones algebraicas surgieron de la aritmética elemental.

La importancia de las estructuras algebraicas, es decir, los conjuntos provistos de una o varias operaciones algebraicas, no reside únicamente en sus aplicaciones en teoría de números. Muchos objetos matemáticos se estudian mediante la construcción de las debidas estructuras algebraicas, que reflejan sus aspectos esenciales. Algo semejante se aplica a los objetos del mundo real.

Con este tema hemos hecho un recorrido por la teoría de grupos, resulta muy útil al investigar por ejemplo las partículas elementales en la mecánica cuántica, las propiedades del cuerpo rígido y los cristales. ●

Bibliografía

DUMMIT D.S., FOOTE R.M. "Abstract Algebra" Prentice-Hall 1991.

SPINDLER K. "Abstract Algebra with applications" Marcel Dekker, NY 1994.

KOSTRIKIN A.I. "Introducción al algebra" McGraww-Hill Iberoamericana 1992.

VERA LOPEZ A., VERA LÓPEZ FCO. J., GARCÍA SÁNCHEZ A. "Algebra Abstracta" 1992.